MGD/HDM:PJC
F. #2021R00440

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

- against -

HUA HUANG,

Defendant.

- X

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS 3902 UNION STREET, #2, FLUSHING, NY 11354, AND ALL LOCKED AND CLOSED CONTAINERS LOCATED THEREIN

- X

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST AND SEARCH WARRANTS

22-MJ-1295

(T. 18, U.S.C., § 1349)

EASTERN DISTRICT OF NEW YORK, SS:

JILLIAN HUSMAN, being duly sworn, deposes and states that she is a Special Agent with the United States Department of Health and Human Services, Office of the Inspector General ("HHS-OIG"), duly appointed according to law and acting as such.

In or about and between November 2021 and November 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant HUA HUANG, together with others, did knowingly and willfully conspire to execute a scheme and artifice to defraud Medicare and Medicaid, health care benefits programs as that term is defined under Title 18, United States Code, Section 24(b), and to obtain, by means of one or

more materially false and fraudulent pretenses, representations and promises, money and property owned by, and under the custody and control of, Medicare and Medicaid, in connection with the delivery of a payment for health care benefits, items and services, contrary to Title 18, United States Code, Section 1347.

(Title 18, United States Code, Section 1349)

The source of your deponent's information and the grounds for her belief are as follows:

1. I make this affidavit in support of an application for an arrest warrant for the defendant HUA HUANG and in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known and described as 3902 Union Street, #2, Flushing, New York 11354 (the "SUBJECT PREMISES"), as more fully described in Attachment A, for the things described in Attachment B, which constitute evidence, fruits and instrumentalities of health care fraud, in violation of Title 18, United States Code, Section 1347, paying illegal kickbacks and bribes, in violation of Title 42, United States Code, Section 1320a-7b(b)(2)(B), conspiracy to commit health care fraud, in violation of Title 18, United States Code, Section 1349, and conspiracy to defraud the United States and pay illegal kickbacks and bribes, in violation of Title 18, United States Code, Section 371 (the "SUBJECT OFFENSES").

2. I have been a Special Agent with HHS-OIG for approximately four years. As an HHS-OIG Special Agent, I investigate health care fraud, including schemes to defraud Medicare and Medicaid and other health care benefit programs. During my tenure with HHS-OIG, I have participated in a variety of criminal health care fraud investigations, during the course of which I have interviewed witnesses, conducted physical surveillance, arranged consensually monitored telephone calls and video recordings, executed search warrants and

reviewed health care claims data, bank records, telephone records, medical records, invoices and other business records. I am familiar with the records and documents maintained by health care providers and the laws and regulations related to the administration of Medicare and Medicaid and other health care benefit programs.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from, among other things: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, and (c) information obtained from witnesses.

4. Except as explicitly set forth below, I have not distinguished in this affidavit between facts of which I have personal knowledge and facts of which I have hearsay knowledge. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of search and arrest warrants, I have not set forth each and every fact learned during the course of this investigation. Instead, I have set forth only those facts, in sum and substance and in part, which I believe are necessary to establish probable cause for the issuance of the search warrant and arrest warrant.

PROBABLE CAUSE

At all times relevant to this Application:

I. The Defendant and the Relevant Entities and Individuals

5. NY Elm Pharmacy, Inc. ("NY ELM") was a retail pharmacy that operated within the SUBJECT PREMISES. NY ELM maintained a bank account ending in 1939 (the "1939 Account") at Financial Institution-1, an entity whose identity is known to me.

6. Pharmacy-1, an entity whose identity is known to me, was a retail pharmacy that operated in Flushing, New York.

7. Individual-1, an individual whose identity is known to me, owned NY ELM and Pharmacy-1. Individual-1 was a signatory on the 1939 Account.

8. The defendant HUA HUANG was an NY ELM and Pharmacy-1 employee.

9. Doctor-1, an individual whose identity is known to me, was a medical doctor who specialized in podiatry and who was enrolled as a Medicare and Medicaid provider. Medicare claims data for claims submitted during the period from approximately November 2021 to November 2022 showed that Doctor-1 ranked third among providers who signed prescriptions that were billed to Medicare by NY ELM, based on the amount paid by Medicare to NY ELM. Medicare claims data for claims submitted during the period from approximately November 2021 to November 2022 showed that Doctor-1 was ranked ninth among providers who signed prescriptions that were billed to Medicare by Pharmacy-1, based on the amount paid by Medicare to Pharmacy-1.

10. Store-1, an entity whose identity is known to me, was a durable medical equipment ("DME") supplier located in Flushing, New York. Individual-1 owned or was associated with Store-1.

II. The SUBJECT PREMISES

11. The SUBJECT PREMISES is a retail pharmacy located at 3902 Union Street, #2, Flushing, New York 11354. It is located within the ground floor of one-story commercial building that has other commercial units. The SUBJECT PREMISES is accessible

through a glass door under a green awning with "NY ELM PHARMACY, INC." and Chinese and Korean symbols written on it. The exterior of the SUBJECT PREMISES is depicted below:

III. Medicare and Medicaid

12. Medicare was a federal health care program providing benefits to persons who are 65 years old or disabled. Medicare was administered by the Centers for Medicare and Medicaid Services ("CMS"), a federal agency under the United States Department of Health and Human Services. Individuals who received benefits under Medicare were referred to as Medicare "beneficiaries."

13. Medicare was divided into multiple parts. Medicare Part B covered outpatient hospital services and professional services provided by physicians and other providers, including DME. Medicare Part C—also known as Medicare Advantage—offered beneficiaries the opportunity to secure coverage from private insurers ("Contractors") for many of the same services that were provided by Part B. Medicare Part D provided prescription drug coverage to persons who were eligible for Medicare.

14. CMS provided fixed, monthly payments to the Contractors for each beneficiary enrolled in a Medicare Advantage plan administered by the Contractors. These monthly payments were referred to as "capitation" payments. To obtain payment for treatment or services provided to a beneficiary enrolled in a Medicare Advantage plan, health care providers submitted itemized claim forms to the Contractors.

15. Medicaid was a federal and state health care program providing benefits to individuals and families who met specified financial and other eligibility requirements, and certain other individuals who lacked adequate resources to pay for medical care. CMS was responsible for overseeing Medicaid in participating states, including New York State. Individuals who received benefits under Medicaid were referred to as "recipients."

16. Medicaid was a health and long-term care coverage program jointly financed by states and the federal government pursuant to the Social Security Act of 1965. Each state established and administered its own Medicaid program and determined the type, amount, duration and scope of services covered within broad federal guidelines.

17. Medicaid covered the costs of medical services and products ranging from routine preventive medical care for children to institutional care for the elderly and disabled.

Service providers were authorized to submit claims to Medicaid only for services they actually rendered and were required to maintain patient records verifying the provision of services.

18. In New York State, Medicaid provided coverage to its recipients for prescription drugs. Medicaid recipients could obtain their prescription drug benefits from pharmacies either through "fee-for-service" enrollment or through Medicaid Managed Care plans, which were administered by private insurance companies that were paid by Medicaid.

19. As part of their insurance benefits, some Medicare beneficiaries and Medicaid recipients received a certain amount of credit per month that could be spent on eligible over-the-counter ("OTC") non-prescription items such as analgesics, diabetes supplies, antihistamines, weight management supplies, sleep aids, vitamins, toothpaste, DME and other items. OTC money could not be spent on items such as cosmetics, hair care products, dry-skin lotions and perfumes. The monthly OTC credit was pre-loaded onto debit cards known as "over-the-counter cards" or "OTC Cards," which were issued to recipients by the plan sponsors. Any funds that were not used by the end of the month were forfeited, and the OTC Cards were reloaded each month with refreshed funds. Pharmacies generally dispensed OTC benefits to recipients by swiping the OTC Cards, like debit cards, through an electronic payment system.

20. Medicare, the Contractors and Medicaid were "health care benefit programs," as defined by Title 18, United States Code, Section 24(b) and referenced in Title 18, United States Code, Section 1347.

21. Pharmacies were typically required to submit claims electronically to Medicare, the Contractors and Medicaid in order to receive reimbursement.

22. By submitting a claim to Medicare, the Contractors or Medicaid, the provider certified, among other things, that the services were rendered to the patient, were medically necessary and were not rendered as a result of kickbacks or bribes.

23. New York State requires pharmacies to keep on file for six years signed prescriptions or fiscal orders for which Medicaid payments are claimed. For deliveries of prescribed medications, delivery confirmation is required to be maintained by a pharmacy for six years from the date of payment. In addition, under these rules, telephone orders from prescribers are required to be reduced to writing and to indicate the time of the call and the initials of the pharmacist.

24. Pharmacists must also maintain for five years on the pharmacy's premises a log, either physical or electronic, reflecting the prescriptions that are dispensed each day, as well as a complete patient medication profile reflecting all medications dispensed to the patient within the last five years.

IV. The Health Care Fraud Conspiracy

25. In or about and between November 2021 and November 2022, the defendant HUA HUANG, together with others, agreed to execute and executed a fraudulent scheme at Pharmacy-1 and NY ELM by which claims were submitted and caused to be submitted to Medicare, the Contractors and Medicaid for the dispensing of pharmaceutical products and DME even though such items were medically unnecessary, procured by illegal kickbacks and bribes and otherwise did not qualify for reimbursement.

26. As part of the scheme, the defendant HUA HUANG, together with others, regularly paid and promised to pay illegal kickbacks and bribes in the form of supermarket gift cards and cash to Medicare beneficiaries and Medicaid recipients in exchange for the ability to

bill Medicare, the Contractors and Medicaid for prescription medications, DME and other services.

27. In or about February 2021, HHS-OIG received an investigative referral related to Pharmacy-1's claims for suspected medically unnecessary high-cost topical prescriptions commonly prescribed in combination and associated with fraud schemes. The referral found similar patterns at two other pharmacies owned by Individual-1. Medicare claims data for claims submitted during the period from approximately January 2018 through July 2022 for prescriptions billed to Medicare by Pharmacy-1 showed that the most prescribed drug at Pharmacy-1 was Diclofenac Epolamine, a pain reliever.

28. In or about and between November 2021 and November 2022, a confidential source (the "CS"),[1] an individual who was a Medicare beneficiary and Medicaid recipient and whose identity is known to me, was a customer of Pharmacy-1 and NY ELM. During that time period, the CS filled prescriptions at Pharmacy-1 and NY ELM.

29. On multiple dates between November 2021 and November 2022, the CS brought prescriptions to Pharmacy-1 and NY ELM. In exchange, Pharmacy-1 and NY ELM employees, including the defendant HUA HUANG, promised and provided the CS with supermarket gift certificates for each prescription filled as well as cash in exchange for his/her monthly OTC benefit, and referred the CS to a doctor who could provide additional prescriptions that Pharmacy-1, NY ELM and Store-1 could bill to Medicare.

[1] This source has been used extensively by HHS-OIG over a period of several years. His/her information has proven reliable and trustworthy and, as set forth below, is corroborated by other evidence obtained in the investigation to date. The source is financially compensated for each undercover operation he/she conducts.

30. On approximately November 29, 2021, CS went to Pharmacy-1 and inquired with the defendant HUA HUANG as to what benefits the CS could receive in exchange for bringing prescriptions to Pharmacy-1. HUANG told the CS that he/she should see the pharmacy's podiatrist and if he/she received prescriptions he/she could receive supermarket gift certificates. The CS asked HUANG about exchanging his/her OTC benefits, and HUANG explained that the CS could receive approximately $150 in cash after the CS saw the podiatrist. HUANG provided a business card to the CS to provide to the podiatrist and explained that the podiatrist would prescribe the CS shoes.

31. On approximately December 8, 2021, the CS returned to Pharmacy-1 and the defendant HUA HUANG asked the CS if he/she had seen Doctor-1 yet. Since the CS had not seen Doctor-1 yet, another Pharmacy-1 employee walked the CS to Doctor-1's office. While there, the CS asked Doctor-1 about the benefits of seeing him. Doctor-1 explained, in sum and substance, that the pharmacy provides benefits, including OTC exchange and supermarket gift certificates. Doctor-1 told the CS, in sum and substance, that he/she has good insurance, so he/she should use it, and further told the CS, "It's not like you don't have a problem and we have to find a problem for you." The CS repeatedly told Doctor-1 that he/she did not have pain in his/her feet, but Doctor-1 told the CS that he/she had nail fungus, which should be treated, and that Pharmacy-1 had suggested pain patches for his/her knee and back. The CS had not told anyone at Pharmacy-1 that he/she had pain.

32. The CS then returned to Pharmacy-1 and provided an employee with a form from Doctor-1. The employee told the CS that the form was for ordering shoes. The defendant HUA HUANG then handed the CS an envelope containing $150, the balance from his/her OTC card. HUANG told the CS to wait a few days for the prescriptions from Doctor-1.

33. On approximately December 17, 2021, the CS went to Store-1 to receive shoes prescribed by Doctor-1. An employee told the CS that he/she could pick any shoes he/she liked. The employee also told the CS that Store-1 was associated with Pharmacy-1. The Store-1 employee told the CS that he/she should see Doctor-1 again in six months to obtain another pair of shoes. The CS then went to Pharmacy-1, where he/she overheard an employee and an unknown customer discussing the fact that Pharmacy-1 had previously retained the customer's OTC card. The CS asked for the prescriptions he/she was prescribed, but an employee told him/her that Pharmacy-1 would deliver them to him/her along with the OTC card.

34. In my training and experience, I have found that pharmacies that provide similar kickbacks and bribes in exchange for the use of patients' monthly OTC benefits often retain their customers' OTC cards on their premises.

35. On approximately January 6, 2022, the CS returned to Pharmacy-1, where he/she received one prescription medication prescribed by Doctor-1. An employee told the CS that Doctor-1 had prescribed additional medications, but those were not covered by the CS's insurance. The CS asked about receiving a supermarket gift certificate for the prescription he/she filled and also about exchanging his/her OTC benefits. An employee took the CS's OTC card and said someone would call him/her.

36. On approximately January 24, 2022, the CS returned to Pharmacy-1. The defendant HUA HUANG reviewed the CS's list of prescriptions on the computer and asked which supermarket gift certificates he/she wanted. HUANG then gave the CS $155 in cash for his/her OTC benefits, which had increased from the $150 the CS had previously been entitled to, and $3 supermarket gift certificates for each of four prescriptions prescribed by Doctor-1, including two boxes of Diclofenac Epolamine, despite the CS not having any pain and there

being no discussion of pain between the CS and employees at Pharmacy-1. The labels for the prescriptions listed "NY ELM" and the address 3426 Union Street, Flushing, New York. The CS asked HUANG if he/she could leave the prescription drugs at the pharmacy, and HUANG told the CS to take them because otherwise they would be thrown away because there were no exchanges.

37. On approximately November 1, 2022, the CS went to the SUBJECT PREMISES, where he/she spoke to the defendant HUA HUANG. HUANG told the CS that NY ELM operations had moved from 3426 Union Street, Flushing, New York, and had relocated to the SUBJECT PREMISES. The CS asked HUANG whether the benefits for filling prescriptions at NY ELM were the same as at Pharmacy-1, and she confirmed that they were. The CS asked HUANG if he/she could exchange his/her OTC benefits. HUANG swiped the CS's OTC card, finding a balance of $155, but she explained that she would not give the CS cash because he/she had no prescriptions to pick up, he/she had not been to the pharmacy in a while and he/she had a high co-payment due.

38. Based on my training and experience, including my investigation of NY ELM, Pharmacy-1 and other pharmacies providing illegal kickbacks and bribes in the form of cash or gift certificates in exchange for OTC benefits, this conversation between the CS and the defendant HUA HUANG suggests a quid pro quo with pharmacy customers whereby a kickback is provided in exchange for prescriptions that are filled at the pharmacy.

39. Medicare and Medicaid claims data for a single Contractor shows that Doctor-1 submitted more than 225 prescriptions for Diclofenac between October 2019 and November 2022 that were filled at Pharmacy-1 or NY ELM, resulting in the payment of approximately $250,000.

40. On numerous occasions that the CS was present at NY ELM and the SUBJECT PREMISES, including on November 1, 2022, he/she observed NY ELM employees using computers to carry out NY ELM's business, including to process and verify prescriptions.

41. The 1939 Account, among other bank accounts controlled by Individual-1, shows more than $900,000 in transfers to and from Pharmacy-1. It also shows more than $85,000 in checks written to multiple supermarkets between approximately February and October 2022. Similar payments to supermarkets during 2018 to 2022 are evident in other bank accounts controlled by Individual-1.

42. Based on my training and experience, and information obtained through this investigation, including the CS's observation that NY ELM has computers in the pharmacy area and uses them when dealing with customers and the fact that similar investigations into pharmacies engaged in similar conduct have involved the use of computers, I believe that NY ELM uses computers to track its customers' medical records and prescription medications, including records of the prescribing medical provider. Based on my training and experience, including investigations into other pharmacies engaged in health care fraud and illegal health care kickback and bribe schemes, these electronic records include information related to billing, co-payments, dispensed OTC benefits and balances, prescription refills and whether a pharmacy received a prescription via phone or electronic submission. NY ELM and other similar pharmacies also use an electronic payment system to charge Medicare beneficiaries and Medicaid recipients' OTC cards, which may be capable of generating a transaction log.

43. Based on my training and experience, including my investigation of other pharmacies that have paid illegal health care kickbacks and bribes to Medicare beneficiaries and Medicaid recipients to induce them to fill prescriptions at the pharmacy, the scheme is carried

out through a referring relationship with a medical provider who is financially compensated for providing prescriptions that the pharmacy can bill to Medicare and Medicaid.

44. Based on the foregoing, there is probable cause to arrest the defendant HUA HUANG for conspiracy to commit health care fraud, in violation of Title 18, United States Code, Section 1349, based on, among other things, her payment of illegal kickbacks and bribes in the form of cash in exchange for OTC benefits and supermarket gift certificates for prescriptions filled at NY ELM and Pharmacy-1 on multiple occasions and her referral of the CS to Doctor-1 for specific prescriptions for medications that were not medically necessary, which were then provided to the CS and subsequently billed to Medicare by NY ELM.

45. Based on the foregoing, there is probable cause to believe that evidence, fruits and instrumentalities of the SUBJECT OFFENSES will be found at the SUBJECT PREMISES, including but not limited to records related to prescriptions filled at NY ELM, supermarket gift cards, financial records related to reimbursement for claims submitted to Medicare and Medicaid for the dispensing of prescriptions that were obtained through the payment of illegal health care kickbacks and bribes and records regarding OTC disbursements.

V. TECHNICAL BACKGROUND

46. As described above and in Attachment B, this application seeks permission to search for records constituting evidence, fruits or instrumentalities of the SUBJECT OFFENSES enumerated here that might be found in the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found, based upon the information obtained in our investigation, is in the form of data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of

computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

47. I submit that if a computer[2] or storage medium[3] is found on the SUBJECT PREMISES, as anticipated based upon our investigation, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a

[2] For purposes of the requested warrant, a computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

[3] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on the facts described above, and other evidence related to this investigation, I am aware that computer equipment was used to, among other things, generate, submit and store documents used in the above-described health care fraud scheme.

48. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file

(such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history and anti-virus, spyware and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media

access, use and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspects. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

49. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the time required for examination, technical requirements, and the variety of forms of electronic media, as explained below:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the SUBJECT PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

50. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would authorize seizing, imaging or otherwise copying computers and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

51. NY ELM is a functioning company that may conduct some legitimate business. The seizure of NY ELM's computers may limit NY ELM's ability to conduct any such legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage

media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of NY ELM so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of NY ELM's legitimate business, if any. If, after inspecting the computers, it is determined that retaining some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return the unneeded equipment.

VI. SPECIAL INSTRUCTION REGARDING REVIEW OF THE SEIZED MATERIAL

52. With respect to law enforcement's review of the seized material identified in Attachment B, law enforcement (i.e., the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and contractors whom law enforcement deems necessary to assist in the review of the seized material (collectively, the "Review Team") shall review, in the first instance, the seized material.

53. If, during the review of the seized material, the Review Team finds potentially privileged materials,[4] the Review Team will: (1) immediately cease its review of the potentially privileged materials at issue; (2) segregate the potentially privileged materials at issue; and (3) take appropriate steps to safeguard the potentially privileged materials at issue. Nothing in this Affidavit shall be construed to require the Review Team to cease or suspend review of all the seized material upon discovery of the existence of potentially privileged materials within a portion of the seized material.

[4] The investigation has not revealed any information suggesting potentially privileged materials may be found at the SUBJECT PREMISES. The discussion of such materials herein is included solely in an abundance of caution.

VII. Request for Sealing

54. I respectfully request that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the instant application and search and arrest warrants. This investigation is not known to the targets, who are currently at liberty, and it is respectfully submitted that sealing these documents is necessary to prevent the targets from learning that a search warrant has been issued, and to thus prevent the targets from avoiding arrest and prosecution and destroying evidence.

Jillian Husman

JILLIAN HUSMAN
Special Agent, HHS-OIG

Sworn to before me this
6th day of December, 2022

Robert Levy

THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The SUBJECT PREMISES is a retail pharmacy located at 3902 Union Street, #2, Flushing, New York 11354. It is located within the ground floor of one-story commercial building that has other commercial units. The SUBJECT PREMISES is accessible through a glass door under a green awning with "NY ELM PHARMACY, INC." and Chinese and Korean symbols written on it. The exterior of the SUBJECT PREMISES is depicted below:

ATTACHMENT B

Particular Things to be Seized

1. All evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1347 (health care fraud), Title 42, United States Code, Section 1320a-7b(b)(2)(B) (paying illegal health care kickbacks), Title 18, United States Code, Section 1349 (conspiracy to commit health care fraud), Title 18, United States Code, Section 371 (conspiracy to defraud the United States and pay illegal health care kickbacks) (the "SUBJECT OFFENSES"), involving the defendant HUA HUANG, DING CHENG YANG ("Doctor-1"), NY Elm Pharmacy Inc. ("NY ELM") and Elmcare Pharmacy Inc. ("ELMCARE" or "Pharmacy-1") from January 2018 to November 2022, and involving the submission of claims for reimbursement to Medicare, the Contractors or Medicaid and the payment of illegal kickbacks, including but not limited to:

(a) Documents constituting, concerning, or relating to payments to patients, in cash, store credit, supermarket gift certificates or otherwise, including cash; documents constituting, reflecting or memorializing store credit earned by NY ELM and ELMCARE customers; gift certificates and other documents constituting, reflecting or memorializing stored or transferrable monetary value; ledgers and other documents identifying Medicare beneficiaries or Medicaid recipients; records reflecting payments made to Medicare beneficiaries or Medicaid recipients, including the amount and date of payments; records reflecting which NY ELM and ELMCARE employees made any such payments; employee records that further identify NY ELM and ELMCARE employees who have made payments to Medicare beneficiaries or Medicaid recipients; any receipts signed by Medicare beneficiaries or

Medicaid recipients and any documents provided to Medicare beneficiaries or Medicaid recipients in connection with their filling of prescriptions at NY ELM and ELMCARE;

(b) Documents constituting, concerning, or relating to pharmacy patient files, bills, invoices, and claims for payment/reimbursement for services or items billed, provided, or alleged to have been provided to patients to include, but not limited to, reimbursement claim forms, explanations of medical benefits, dispensing orders, detailed written orders and prescriptions, prior authorizations and supporting materials, certificates of medical necessity, signature logs, dispensing logs, information from physicians concerning the patients' diagnosis, patient transportation records, supply purchases, and proof of delivery of services, items or equipment that were submitted by, NY ELM and ELMCARE, or any representative acting on behalf of NY ELM and ELMCARE, to a health insurance provider for reimbursement;

(c) All business cards pertaining to medical providers, including but not limited to DING CHENG YANG;

(d) All documents and correspondence constituting, concerning or relating to efforts to collect, or the decision to waive, co-payments and/or deductibles for individuals who filled prescriptions at NY ELM and ELMCARE;

(e) All correspondence and cancelled checks relating to notice of overpayment and request for refunds from a health insurance provider;

(f) All correspondence to and from a health insurance provider to or from HUA HUANG, NY ELM, ELMCARE or any of its employees or agents, including, but not limited to, manuals, advisories, newsletters, bulletins, and publications related to illegal health care kickbacks and referring relationships;

(g) All correspondence to and from patients regarding prescription drugs that are medically unnecessary, procured by illegal health care kickbacks and bribes or ineligible for reimbursement, and/or any health insurance or medical provider related to illegal health care kickbacks and referring relationships;

(h) All documents pertaining to and all correspondence to and from DING CHENG YANG;

(i) All contracts, agreements, logs, lists or records related to any payments for medical professional services or referrals for such services, including but not limited to records of payment by the defendant HUA HUANG, NY ELM, ELMCARE or any other NY ELM or ELMCARE employee to any medical provider;

(j) All documents pertaining to fraud, waste and abuse training received by any employee, owner or affiliated person of NY ELM and ELMCARE;

(k) All employee files and resumes of the defendant HUA HUANG, or any other NY ELM or ELMCARE employee. This may include, but is not limited to, time cards/time sheets, payroll records and any documents or computer files listing any and all employee names addresses, telephone numbers, professional licensing and background information for all current and former employees;

(l) Over-the-counter cards kept on file for Medicare beneficiaries and Medicaid recipients;

(m) Financial books and records, including but not limited to:

i. bank accounts, money market accounts, checking accounts, investment accounts, stock fund accounts, 401K funds, mutual funds, retirement funds, employee payment records, tax forms and records, and bonds or bond funds, including deposits and

disbursements, cancelled checks or draft electronic transfers, ledgers, loan statements, loan agreements;

ii. credit card/ATM/debit cards, including but not limited to account statements and physical cards; and

iii. receipts for anything of value provided to Medicare beneficiaries or Medicaid recipients who filled prescriptions at NY ELM and ELMCARE;

(n) All pharmacy records required to be maintained by federal, state or local regulation;

(o) Computers[1] or storage media[2] that contain records or information (hereinafter "COMPUTERS") used as a means to commit the SUBJECT OFFENSES. All information obtained from such COMPUTERS will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. For any COMPUTER whose seizure is otherwise authorized by this warrant, and any computer that contains or in which is stored records or information that is otherwise called for by this warrant:

i. evidence of who used, owned or controlled the COMPUTERS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

---

[1] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers and network hardware, such as wireless routers.

[2] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs and correspondence;

ii. evidence of software that would allow others to control the COMPUTERS, such as viruses, Trojan horses and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence of the attachment to the COMPUTERS of other storage devices or similar containers for electronic evidence;

v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

vi. evidence of the times the COMPUTERS were used;

vii. evidence of the COMPUTERS being remotely accessed or remotely accessing other computers;

viii. passwords, encryption keys and other access devices that may be necessary to access the COMPUTERS;

ix. documentation and manuals that may be necessary to access the COMPUTERS or to conduct a forensic examination of the COMPUTERS; and

x. contextual information necessary to understand the evidence described in this Attachment.

all of which constitute evidence, fruits and instrumentalities of the SUBJECT OFFENSES.